1

Crafting Defense R&D Policy in the Anti-Terrorist Era

Manuel Trajtenberg, *Tel Aviv University, NBER, and CEPR*

Executive Summary

This paper seeks to analyze the nature of the terrorist threat following September 11, 2001, and to explore the implications for defense R&D policy. First, it reviews the defining trends of defense R&D since the Cold War and brings in pertinent empirical evidence. During the 1990s, the United States accumulated a defense R&D stock ten times larger than any other country and almost thirty times larger than Russia. Big weapons systems, key during the Cold War but of dubious significance since then, still figure prominently, commanding 30 percent of current defense R&D spending, vis-à-vis just about 13 percent for intelligence and anti-terrorism. The second part of the paper examines the nature of the terrorist threat, focusing on the role of uncertainty, the lack of deterrence, and the extent to which security against terrorism is (still) a public good. Drawing from a formal model of terrorism that I developed elsewhere (Trajtenberg 2003), I explore these and related issues in further detail. Two strategies for confronting terrorism are considered: fighting terrorism at its source and protecting individual targets (the latter entails a negative externality). Contrary to the traditional case of national defense, security against terrorism becomes a mixed private/public good. A key result of the model is that the government should spend enough on fighting terrorism at its source to nullify the incentives of private targets to invest in their own security. Intelligence emerges as the key aspect of the war against terrorism, and accordingly R&D aimed at providing advanced technological means for intelligence is viewed as the cornerstone of defense R&D. This entails developing computerized sensory interfaces and increasing the ability to analyze vast amounts of data. Both have direct civilian applications, and therefore the required R&D is mostly "dual use." Indeed, there is already a private market for these systems, with a large number of players. R&D programs designed to preserve this diversity and to encourage further competition may prove beneficial both for the required R&D and for the economy at large.

I. Introduction

The devastating terrorist attacks of September 11, 2001, and their aftermath pose a formidable challenge to U.S. national security and call for the rethinking of established dogma in a wide range of fields. The attacks came after a relatively peaceful decade that constituted an interlude between the Cold War and the emerging terrorist threat. Defense R&D had proceeded over the post–World War II decades along the familiar path of the arms race in the nuclear age, bounded only by treaties that sought to mitigate the spiraling costs and preserve the logic of the "mutually assured destruction" doctrine. This coincided with a golden era of scientific and technological progress, unleashing extraordinary advances in military technology.[1] The collapse of the Soviet Union, brought about in part by that same race, left the United States as the only superpower, particularly in terms of its edge in military technology. The new terrorist threat negated much of that advantage, however, because the enemy could neither be effectively deterred by overwhelming military force, nor could it be destroyed by actually deploying that force. In the meantime, defense R&D continued by and large along the old path, still devoting large amounts of resources to the development of big, complex offensive weapons systems that have no rival in the world and for which there is no clear threat that these costly weapons could forestall. A fresh look at defense R&D policy is thus called for, starting from a thorough analysis of the new terrorist threat and seeking to trace its implications for the required R&D. The main goal of this paper is to deploy some basic tools of economic analysis to this much-needed reassessment.

Section II characterizes in detail defense R&D before September 11, 2001, bringing in data to bear both on the total stock of military R&D of the United States vis-à-vis other leading countries and on the composition of R&D spending. Simple computations of the defense R&D stock generated during the 1990s indicate that during that decade alone the United States accumulated a stock ten times as large as that of any other country, and almost thirty times larger than its old foe, Russia. Within this vast technological reservoir, big weapons systems still figure prominently, commanding about 30 percent of current R&D spending (not including the ballistic missile defense program, which commands another 15 percent). On the other hand, R&D aimed at intelligence and anti-terrorism, which the analysis below places at the forefront of the desirable defense R&D policy, constitute only about 13 percent of the known total.

Section III examines the nature of the terrorist threat, focusing on the role of uncertainty, the lack of deterrence, and the extent to which providing security against terrorism is still a public good. This latter issue receives a more detailed treatment in Section IV, where I bring in insights from a formal model of terrorism that I developed elsewhere (Trajtenberg 2003). The building blocks are cast in terms of the probability that a terrorist attack will take place and the (conditional) probability that any particular target will be hit. Two strategies are available to combat terrorism. The first consists of fighting terrorism at its source, thus reducing the overall probability that an attack will take place; this constitutes a public good and hence is to be provided by the government. The second entails potential targets investing in their own security, thus reducing the probability that they will be hit but raising it for others (a negative externality). Contrary to the traditional case of national defense, the provision of security against terrorism thus becomes a mixed private/public good. A key result of the model is that the government should spend enough on fighting terrorism at its source to nullify the incentives of private targets to invest in their own (local) security. The model also allows exploration of the relative impact of R&D aimed at improving the effectiveness of spending on each type of strategy.

Section V attempts to draw implications for the design of a coherent defense R&D policy that would fit the changing nature of the threats facing the United States, and in particular the characterization of the terrorist threat as discussed in Sections III to IV. Intelligence (in the broad sense) emerges as the key aspect of the war against terrorism, and thus R&D aimed at providing advanced technological means for improved intelligence is viewed as the cornerstone of defense R&D. Basic R&D for target-specific protection from terrorist threats, R&D to counter nonconventional threats, and cyber security are additional important aspects of such policy.

Section VI looks into the technological directions implied by the required anti-terrorist R&D and the implications for competition in the relevant markets. The provision of advanced means for intelligence and for target protection entails emulating human sensory perceptions through computerized sensory interfaces and increasing dramatically the ability to analyze in real time vast amounts of information. Both have clear and direct civilian applications, and therefore the required R&D is mostly "dual use." The development of big weapons systems during the Cold War led to a high concentration of both R&D and procurement into a few large corporations, conferring on them a great

deal of market power. By contrast, the development of sensory computer interfaces, Internet security, biological protection, and the like, entails an entirely different playing field. As stated already, these systems are dual use. There is (also) a private market for them, and there exists already a large number of players that can partake in the required R&D. New R&D programs could be designed to preserve this much needed diversity and to encourage further competition. Such programs may prove highly beneficial both for the required defense R&D and for the advanced sectors of the economy themselves, thus fostering economic growth. Section VII concludes with a summary of the principles upon which defense R&D policy for the anti-terrorist era could be articulated.

II. Defense R&D: Before and After September 11, 2001[2]

Since the 1950s and up to the 1990s, the predominant security threat facing the United States was of course that posed by the former Soviet Union, a threat that led to a relentless arms race. The main goal of the U.S. military was, accordingly, to deter the former Soviet Union from attacking the United States or its allies (primarily western Europe), and if attacked, to be able to defeat any combination of threatening states (i.e., including the Warsaw pact members).[3] Defense R&D thus had very clear goals, there was a well-defined (leading) foe, and the rules of the game were also well defined, evolving rather slowly throughout the dynamic interaction with the former Soviet Union.[4] This led to the building of a formidable defense R&D complex, including DARPA, federal labs (such as Livermore, Argonne, and Oak Ridge), large private contractors (such as Lockheed, Grumman, and Raytheon), research at major universities (such as MIT and Stanford), and the R&D performed at the various branches of the military itself.

Throughout the second half of the twentieth century, this vast complex developed ever more powerful and accurate weapons, and in particular big weapons systems such as nuclear devices, intercontinental ballistic missiles, nuclear submarines, large carriers, high-performing aircraft (including jet fighters, large transport planes, combat and transport helicopters, and stealth aircraft), and so forth.[5] The logic of the Cold War arms race dictated to a large extent the direction of R&D. For example, the prevalent mutually assured destruction (MAD) doctrine necessitated the development of nuclear subs that could survive and operate autonomously even after a devastating nuclear attack on the

mainland United States and deliver a retaliatory blow on the enemy. Conversely, various treaties with the former Soviet Union limited the development of antiballistic missiles.[6]

Fortunately for all involved, the logic of the MAD doctrine worked well, and the immense arsenal of highly sophisticated and lethal weapons (in particular the big weapons systems) developed during the Cold War remained for the most part unutilized. A relentless arms race terminated without a major confrontation, essentially by the internal (but not unrelated) collapse of one of the contenders. However, the enormous R&D resources poured into the development of those weapons systems over decades did achieve their goal: to deter a major armed conflict. In that sense, the relative peace in which the American people and most of the world lived for half a century owes as much to defense R&D as to anything else.

The collapse of the former Soviet Union shattered the basic premises that had guided defense R&D primarily because a foe having commensurate capabilities and racing for parity or supremacy no longer existed. Thus, attention gradually shifted away from the prospect of an all-out war to regional conflicts in which the United States may have a stake as well as to issues stemming largely from the split-up of the Soviet Union, such as preventing nuclear leakage. A common denominator of these new challenges was that the mighty deterrence built over the decades of the Cold War was no longer effective, if only because the United States could not conceivably resort to a nuclear strike against foes that did not pose a commensurate threat to the United States itself. Defense R&D was thus to serve new goals, such as the ability to fight simultaneously two regional conflicts (emphasizing rapid deployment, maintainability of equipment, etc.) and to minimize casualties in any confrontation (one of the legacies from the Vietnam War). Yet throughout the 1990s, a big chunk of defense R&D was still devoted to big weapons systems, such as the development of new high-performing and extremely expensive aircraft. Indeed, and perhaps not surprisingly, defense R&D exhibited a large degree of inertia, partly as a consequence of the fact that R&D expenses grow rapidly as a project moves forward from basic research toward development, testing, and evaluation. Thus, "legacy" projects that were conceived a decade or more earlier proceeded to absorb increasing R&D resources over time, even though the need for them had almost vanished.

Much as the fall of the Soviet Union over a decade earlier marked the closing of an era, September 11, 2001, signified the beginning of a

new one, one dominated by the worldwide terrorist threat (see Hoge and Rose 2002). Of course, large-scale terrorism against the United States did not start with the attack on the World Trade Center (WTC) and the Pentagon; the devastating attack on the U.S. marine barracks in Beirut in 1983, the attacks on the U.S. embassies in Nairobi and in Dar es Salaam in 1998, and the attack on the U.S.S. Cole in October 2000 were painful indications of the evolving new threat. Yet September 11, 2001, was qualitatively different because it was the first large-scale attack on the homeland, an attack of a far larger magnitude than anything done before. Indeed, September 11, 2001, was the equivalent of a declaration of war, of total war, on the United States. It was a declaration of war by a diffused, amorphous enemy who did not put forward a clear set of demands, or even a well-defined set of grievances that could be negotiated away, or mitigated. The nature of the threat and the accompanying challenge to the United States security are thus unprecedented.

The shock caused by September 11, 2001, can be seen as a combination of Pearl Harbor and Sputnik: a surprise attack resulting in initial stunning losses, the revelation of an unbearable degree of vulnerability, the birth of a major new threat to national security, and the dearth of technological means to face it effectively. The latter is the key to the redesign of a coherent defense R&D policy because we have once again a well-defined goal, namely, the development of the scientific and technological infrastructure to serve the long-term war against terrorism. This goal has far-reaching implications in terms of the direction of the defense R&D, and if pursued forcefully, it would represent a significant departure from the kind of R&D done until September 11, 2001. Before analyzing in more detail what the war on terrorism requires, it is important to note what is *not* needed in this new era, thus suggesting a policy that involves primarily a re-allocation of existing resources rather than increased expenditures.

Defense R&D Stocks

Following the collapse of the Soviet Union, there is no country (or plausible coalition of countries) that can challenge the present technological supremacy of the U.S. military.[7] Indeed, the defense R&D stock of the United States, developed and accumulated over the past decades, is far larger than that of any country in the world.[8] The only other sizable stock was that of the former Soviet Union, but that has shrunk dramatically after the collapse, and Russia cannot afford to renew it.[9] Japan has severe built-in constraints on spending for defense R&D, making it a noncontender for the foreseeable future. Western Europe has advanced technological capabilities but has spent less than the United States for the past decades and, barring a dramatic geopolitical change, it will continue its spending rate in the future.

Table 1.1
Defense R&D stock as of 2000 (in billions of constant 1998 $ U.S.)[a]

	Stocks based on a depreciation rate of:	
G8 countries	15%	5%
United States	197.23	301.64
United Kingdom	18.21	28.03
France	17.81	28.69
Japan	9.96	14.78
Germany	9.18	13.47
Russia	7.14	11.06

[a]The data used in these computations are given in appendix 1.1. Note that there is a significant degree of uncertainty regarding some of these data, particularly for Russia. Thus, these figures should be taken as indicative only. To compute the stocks, I simply apply the following formula: $\Sigma_{t=0}^{9} D_{1991+t} \cdot (1 - r)^{9-t}$, where D_{1991+t} denotes defense R&D expenditures in year 1991 + t.

To gain an idea of the actual magnitudes involved, I computed the defense R&D stocks generated during the decade of the 1990s (1991–2000) for the G8 countries that have had significant military R&D investments.[10] These are not the *total* stocks available but only the portion added during the 1990s. These countries (particularly the United States) had substantial defense R&D stocks prior to that decade, which were generated during the long decades of the Cold War. As table 1.1 reveals, during the 1990s, the United States accumulated an additional defense R&D stock over ten times as high as the next largest (the United Kingdom, if we use a depreciation rate of 15 percent), twenty-eight times that of Russia, and over three times that of the other countries combined. These differences are stunning and give a quantitative sense of the technological supremacy of the United States referred to above.

Some qualifications to these computations are in order. First, table 1.1 quite likely overstates the actual technological gap between the United States and its allies because the United States exports to them military equipment embedding technological advances achieved by

the R&D that goes into these stocks, and some of the R&D projects are joint with them. On the other hand, the extent of underreporting of defense R&D (due to secrecy—these are the so-called "black programs") is likely to be significantly higher in the United States than in western Europe. Second, there are likely to be spillovers and leakages from the defense R&D done in the United States that enhance the technological capabilities of other countries. It is hard to believe, however, that these qualifications would alter significantly the picture that emerges from table 1.1.

Beyond the advanced nations, China is perhaps the only emerging power that may be a source of concern. A simple calculation indicates, however, that the possibility of China posing a serious challenge to the defense R&D advantage of the United States is rather unlikely. The United States spends about 0.4 percentage points of its GDP on defense R&D. China's GDP is about one-tenth that of the United States; thus, to match the U.S. current level of spending, China would have to allocate a staggering 4 percent of its GDP to defense R&D and maintain that level for many years, a rather far-fetched scenario.[11] Furthermore, matching on a current basis would erase the initial huge advantage of the United States only in the very long run. Essentially, the vastly larger economic resources of the United States vis-à-vis any other nation, and the fact that it already possesses a huge stock of military R&D, gives the United States an unmatched technological advantage that cannot be challenged unless a dramatic geopolitical change occurs. Even if that were the case, however, the United States would still have significant margins of time (and resources) to respond.

The Composition of Defense R&D

How much does the United States invest in R&D aimed at big weapons systems versus other technological means that could help confront current threats to national security? To address this issue, I examine in detail the composition of the defense R&D budget for fiscal years 2001 to 2003. The Office of the Under Secretary of Defense (Comptroller) publishes a document called "RDT&E Programs" that contains almost 800 budget items, indicating the agency in charge, the type of program, the program name, and the allocated budget. (See appendix 1.2 for a list of the top twenty items in the list.) With the aid of expert officers of the Israeli air force, we managed to classify 369 of the 798 items

listed, which account for about 90 percent of the budget.[12] The categories used were:

- B—big weapons systems
- D—ballistic missile defense
- I—intelligence
- T—anti-terrorism
- M—miscellaneous (i.e., not classified elsewhere)

By "big weapons systems," I mean traditional, large, complex weapons systems having mostly an offensive character, such as jet fighters, ICBMs, carriers, nuclear submarines, and the like. We created a separate category for ballistic missile defense, because these are *defensive* systems that are relatively new and meant to respond to present and future threats posed by the proliferation of long-range missile technologies in potentially hostile states. In case of doubt between "B" and "M," we opted for "M" to prevent biasing the totals in favor of the argument put forward here. Intelligence is almost certainly underrepresented in these data, if only because the funding of the Directorate of Science and Technology of the CIA is not included in these figures (as far as I know). The "T" category is almost surely understated as well because it is very hard to discern what exactly qualifies as "anti-terrorism." As it stands now, it includes all items related to chemical and biological warfare,[13] and a few others.[14] The newly created Department of Homeland Security presumably commands additional budgets for anti-terrorism-related R&D that are not included in our figures. "Miscellaneous" means "not classified elsewhere"; that is, it is the default category for all items that do not clearly belong into one of the others. Significant margins of error likely remain in the classification performed, and intelligence and anti-terrorism, in particular, are quite certainly downward biased; however, I hope that the summary results presented in tables 1.2 and 1.3 are still informative and in the right ballpark.

As tables 1.2 and 1.3 reveal, about 30 percent of the reported defense R&D is (still) allocated to big weapons systems. This category includes the development of systems that have no rival in the world, and it is not clear what sort of security threats these costly weapons are meant to forestall. The prime example is the F-22, a kind of technological marvel. It is an extremely expensive aircraft, with projected capabilities

Table 1.2
Distribution of defense R&D: 2001–2003 (current thousand $)

Category	FY 2001	FY 2002	FY 2003
Big weapons systems	10,752,781	11,911,890	13,805,069
Miscellaneous	12,107,023	14,029,675	14,407,247
Ballistic missile defense	4,302,183	7,039,441	6,848,958
Intelligence	2,953,072	3,378,629	4,490,930
Anti-terrorism	754,140	902,937	1,394,472
Not classified	4,497,512	4,081,025	4,178,031
Total[a]	***35,366,710***	***41,343,596***	***45,124,706***

[a]The total amounts here are lower than the total defense R&D budgets by about 10 to 15 percent. Defense-related R&D done by other government agencies (such as NIH) is not included; there are other, apparently classified items not reported in the published list, and some of the items listed in the cited document have not been assigned a dollar amount.

Table 1.3
Distribution of defense R&D: 2001–2003 (percentages)

Category	FY 2001	FY 2002	FY 2003
Big weapons systems	30.40	28.81	30.59
Miscellaneous	34.23	33.93	31.93
Ballistic missile defense	12.16	17.03	15.18
Intelligence	8.35	8.17	9.95
Anti-terrorism	2.13	2.18	3.09
Not classified	12.72	9.87	9.26
Total	***100.0***	***100.0***	***100.0***

Source: U.S. Government (2002).

beyond what could be regarded as real needs that current jet fighters could not appropriately fulfill.[15] On the other hand, intelligence and anti-terrorism command only about 10 to 13 percent of the budget.[16] As I argue later, even if the true figures are significantly higher than these, the percentage allocated to these key activities is still quite low, relative to their present and future importance for national security. Therefore, it seems that the dramatic shift in the nature of the threats to national security since September 11, 2001, have had little impact so far on the composition of R&D, and that calls for a prompt revision. One mitigating factor, however, may simply be time. Even if policy priorities shift, it takes a while to implement the desired changes, and in particular, it takes time to launch R&D programs to serve those changing priorities. As figure 1.1 reveals, it took about three years to

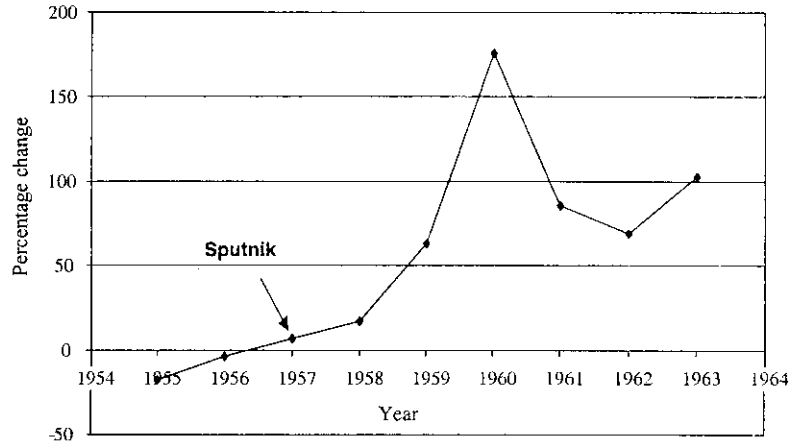

Figure 1.1
NASA R&D expenditures yearly percentage changes: 1955–1963.
Source: Mowery and Rosenberg (1989), table 6.12, pp. 161–165.

beef up NASA's budget after Sputnik—and it has not been three years yet since September 11, 2001.

III. The Nature of the Terrorist Threat

Present-day terrorism, as manifested most potently on September 11, 2001, and since, poses a very different set of threats than the conventional, nation-against-nation type of conflicts that have been prevalent throughout most of history.[17] Confronting such novel threats presents a formidable challenge at all levels: to the current military, intelligence, and police capabilities of the target countries; to their democratic institutions that need to strike a delicate balance in pursuing this war; and also to the scientific and technological resources that need to be mobilized to devise the appropriate technological means to combat terror. The latter requires the design of a coherent and well-articulated R&D policy, which should be based on the systematic analysis of the nature of these threats, in and of themselves, and in contrast to those posed by conventional conflicts. The goal of this section is thus to set the framework for such analysis and in particular to try to identify the distinguishing features of the terrorist threat that have salient implications for R&D policy.[18]

Let me start with two general points. The first is that present-day terrorism is based on and exploits huge asymmetries between the perpetrators and the victims: asymmetry in the perceived value of life (leading inter alia to suicidal attacks), asymmetry in the means of combat (relatively simple for terrorists, highly sophisticated and powerful for the target countries), asymmetry in the information available on each side (mostly open information on the potential targets/victims versus highly secretive, compartmentalized behavior of terrorists), and so forth. That scenario is not true (for the most part) in conventional conflicts between countries, and therefore a great deal of the capabilities accumulated in any country in the course of contemplating or having been engaged in such conflicts, are rendered ineffective for the war on terror. In particular, many of the weapons systems developed by the leading industrialized nations during the twentieth century, and in particular those developed in the course of the Cold War, are not appropriate for fighting terrorism. Thus, R&D policy in this context will have to depart from established premises and offer novel options.

The second observation is that one cannot expect a clear, decisive victory in the war on terror that would defeat the enemy once and for all. Furthermore, in this kind of war there is no possibility of circumscribing the contest, the race, with formal agreements or treaties such as those that were concluded with the former Soviet Union during the Cold War. Therefore, one should proceed on the premise that this will be a protracted confrontation entailing long-term, persistent threats. Accordingly, R&D aimed at it should be multilayered in time, in the sense of being able to generate technological responses for the short, medium, and long term. I turn now to more specific characteristics of the terrorist threat: the key role of uncertainty, limited deterrence, and the private versus public good aspects of providing security in this context.

The Role of Uncertainty

A key feature of the terrorist threat is its generalized, diffused nature, that is, the large degree of uncertainty regarding where, when, and how terrorists may strike. Such uncertainty is what greatly magnifies the terrorist threat, far beyond what it would take to confront the terrorists if faced with them or the actual damage that any single terrorist strike may cause. Indeed, if the authorities had advance knowledge of the timing and location of a future attack, actually thwarting it would be a relatively minor affair involving the deployment of little police or military power.[19]

That is not the scenario in conventional warfare. Confronting, say, an invasion by a foreign power necessitates vast military capabilities, even if one knows when and where the attack will take place. The same applies to a nuclear confrontation. The MAD doctrine required that each party had the capability to nearly annihilate the other, regardless of being able to know in advance the timing and exact targets of an attack. In other words, the sine qua non to fight a conventional or even a nuclear war is a powerful army, measured by the strength and technological means available to its forces. In the end, conventional and nuclear wars are decided by the outcome of the actual clash between the rival armies.[20] By contrast, fighting terrorism involves first and foremost reducing uncertainty, avoiding surprises. If we knew where, say, al Qaeda cells are, apprehending or destroying them would be a relatively easy task. Likewise, if we could detect terrorists as they try to approach or enter a target, then neutralizing them should be the easy part. Even narrowing down the geographical area and/or the approximate time of a possible terrorist strike can greatly simplify the task of thwarting the attack.

The inherent uncertainty of the terrorist threat is also what exerts a heavy price on the threatened nation, far beyond the actual damage that may be inflicted once the attack occurs. Individual terrorist acts or even a series of them may not compromise national security at large, in the sense of hurting a large proportion of the civilian population, damaging a significant chunk of the economy, or (to take it to an extreme) posing a danger of losing sovereignty to a foreign power or to an alien extremist group. And yet the uncertainty about when and where these acts may occur may have far-reaching effects, both in terms of economic costs (e.g., the provision of security at many potential targets; reduced investments because of generalized uncertainty; disruption of travel, tourism, and perhaps also trade) and psychological costs (e.g., painful changes in established norms, behaviors, and "way of life," like the invasion of privacy for the sake of prevention, avoidance of skyscrapers, reduced travel and tourism, etc.). It is precisely because of the uncertainty that accompanies the terrorist threat, and the associated costs, that few terrorists, armed with relatively primitive means, can effectively threaten even the most powerful of countries.

Limited Deterrence

Two of the novel and most disturbing aspects of present-day terrorism are the fact that the perpetrators are ready to commit suicide to fulfill their mission and also the fact that some of their attacks are based on suicide (as was the case for September 11, 2001). Indeed, there is a huge difference between readiness to die for a cause but still hoping to get away alive, and planning from the start to commit suicide in the course of the attack and incorporating that plan as an integral and unavoidable part. Perhaps the most serious implication of the latter is that the possibility of deterrence is greatly reduced, at least in the sense that the perpetrators have nothing to fear for themselves. There still might be some deterrence possible if, for example, the terrorists were based in a sympathetic host country (as was the case with Afghanistan), and hence the victim could retaliate against the host country, or if terrorists had families or wider social networks in known places that could be affected after the fact. However, after the war in Afghanistan, that sort of deterrence seems to be less possible.

Limited deterrence implies that there is little use for offensive weapons systems that in conventional confrontations would be perceived by the potential attacker as posing an *ex post* threat. Thus, suicidal terrorism almost completely neutralizes the initial advantage that advanced countries (the potential victims of terror) had in terms of military might because such military capabilities are rendered ineffective by denying their deterrence value.

National Security: Still a Public Good?

National defense (or national security) has been traditionally regarded as the prototypical type of public good.[21] This is not just a definitional matter but has far-reaching normative implications. Given the "pure" public good nature of defense, economic logic dictates that governments should be in charge of supplying it and in fact should do so exclusively. This provision of defense may be one of the main justifications for the very existence of a government, even in societies patterned after strict market principles. Indeed, defense ranks higher as a public good than, say, maintaining law and order because the latter could be provided by local communities in a decentralized fashion (as has been the case in many instances throughout history). For a given political entity as a whole (e.g., nation, state), however, defense can hardly be

decentralized. Let me restate those aspects of a good or service that make it public rather than private.[22] First, public goods are said to be *nonrival* in consumption; that is, the total amount of the good produced can be "consumed" by each and every individual in society. By contrast, the total amount of a private good produced is divided among consumers, so that if one consumes more, others necessarily consume less. Second, agents providing a private good can prevent others from gaining access to the good and consuming it (for example, excluding those that refuse to pay for it), whereas there are no effective exclusion mechanisms for public goods. It is hard or impossible to prevent anybody that so desires from gaining access and enjoying the public good.

If one thinks of national defense as protection from foreign threats that may in principle affect the country as a whole, it is clear that the two attributes of public goods hold strictly for it: (1) nonrivalry (each citizen enjoys the *full* amount of defense produced), and (2) it is impossible to exclude citizens who, say, don't pay taxes from enjoying the protection from foreign threats offered by the defense capabilities supplied in the country. As the discussion below indicates, however, the nature of defense is much more complex in the context of the war against terrorism.

As already mentioned, a key feature of terrorism is that the threat is generalized (i.e., it can happen anywhere, anytime), and yet any particular attack is local because it entails striking at a particular location that constitutes, even in the worse of cases, a small fraction of the country as a whole. Accordingly, confronting terrorism entails two very different strategies. The first consists of fighting the terrorist threat at its source, namely, intelligence gathering, pinpointing strikes at terrorist cells, denying bases in countries abroad, etc. The second strategy entails deploying resources to protect likely targets in the homeland. It is intuitively clear that the first strategy does retain the public good nature of defense, whereas the second strategy makes the provision of defense mostly a local public good, even conveying negative externalities.

Consider, for example, the threat of terrorist bombings against civilian targets in the form of (local) public places that attract large numbers of people, such as shopping malls or big office buildings. In the absence of specific information on when and where the attack may take place, protecting against such threat involves setting up some form of security system at each such location. That security system may take the form of security guards, checks on each person entering the facility,

metal detectors, "sniffing" machines for luggage (which detect explosives by the chemical fumes they generate), and so forth. Clearly, the deployment of a security system of that sort at a specific potential target location serves first and foremost those present at or otherwise associated with that location, thus making it a local public good. Increasing security at one particular location may actually increase the risk to adjacent locations because terrorists are likely to prefer the least protected target—this is the negative externality mentioned above.[23]

In the case of airports, the issue is more complex, as was painfully realized on September 11, 2001. Most of the victims were located far away from the departure sites and had nothing to do with air travel. In fact, securing airports serves a much wider purpose than just protecting those directly associated with them, and hence it is surely closer to a public good. In the case of public utilities, the effects of a terrorist attack may also be much wider in scope than those occurring at the plant itself and its immediate surroundings. As these examples reveal, there is actually a wide spectrum of possible cases, ranging from strictly local targets to those that may serve just as entry points for more generalized threats, to targets where attacks may have widespread repercussions. I focus in the analysis on just the polar cases to sharpen the issues at stake, but we should keep in mind that actual threats may lie somewhere between.

These qualifications notwithstanding, terrorism has indeed caused national security to become partly a private good. Therefore, the provision of defense is no longer strictly confined to the government but has been to some extent privatized. Of course, security in general (e.g., protection from local crime such as theft, violence, sabotage, and industrial espionage) has always been to some extent privately supplied, and there is indeed a sizable cottage industry already in place that supplies it. In that sense, the tension between the two strategies described above may be seen as a replay of the tension that may exist in any urban center between, say, preventive police action, on the one hand, and placing private guards or security systems at specific locations, on the other. Of course, huge differences exist between terrorism and traditional forms of crime. Those differences have to do primarily with the relative magnitude of the threats, the underlying causes and ultimate aims of each, and the national (and even cultural) significance of the threats. These differences surely enhance the role of the government in protection from terrorism versus traditional crime, and yet wide margins exist for the private provision of security. Distributional considerations for government intervention are surely more compelling in the case of terrorism.[24]

IV. Sketching a Model of Terrorism

I have developed elsewhere (Trajtenberg 2003) a formal model of terrorism that allows one to analyze the various strategies available for confronting the threat of a terrorist attack, the incentives to invest in each by private parties and by the government, R&D aimed at improving the effectiveness of these strategies, etc.[25] Following a sketchy description of the building blocks of the model, I present some of the inferences that can be drawn from it and that are of particular relevance for R&D policy.

The model starts by analyzing the behavior of the three parties involved in the "game" of terrorism: (1) the terrorists, whose aim is to inflict damage to potential targets, and hence their "utility" is a positive function of the losses suffered by their victims; (2) the potential targets, who, without terrorism, would go about their business as usual and receive a certain payoff (e.g., profits, rents), but under the threat of terrorism have to factor in the risk of being hit, losing the payoff, and incurring a further loss; and (3) the government, which is interested in minimizing the expected losses from possible terrorist attacks. The cornerstone of the model is the decision-making problem facing the terrorists: they have to decide whether or not to strike, and if they do, then which target to hit. This decision generates a set of probabilities over those possible actions. Potential targets can affect those probabilities through decisions about how much to invest in their own security. Finally, the government decides how much to invest in fighting terrorism at its source, taking into account the behavior of the other parties. The decision of terrorists can be represented by a decision tree, as shown in figure 1.2.

As mentioned in the preceding section, two basic strategies can be used to confront the terrorist threat: (1) fight terrorism at its source, which means in this context undertaking activities that decrease the probability p that an attack will take place (I shall refer to it as the "*S*-strategy," "*S*" for source); and (2) protect particular targets, thus reducing the probability π_i that they will be hit if the terrorists decide to strike (the "*L*-strategy," "*L*" for local). Not surprisingly, the analysis shows that it is highly unlikely that private parties (i.e., individual targets) would be willing to contribute voluntarily to the *S*-strategy, and

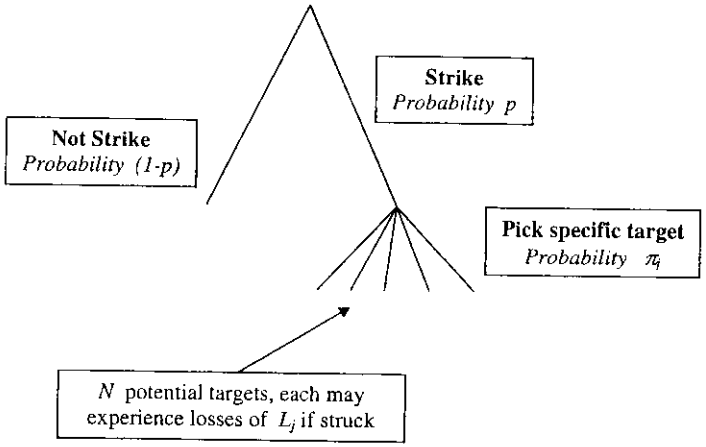

Figure 1.2
The terrorist decision tree.

hence that role is typically left to the government. On the other hand, it is quite likely that each potential target will have enough incentives to spend on the *L*-strategy, which will happen when the expected losses of each target, the probability that terrorists will strike, and/or the effectiveness of private security spending are sufficiently large (in a sense made precise in the model). The provision of security against terror then takes a dual nature: a public good, on the one hand (i.e., reducing the likelihood of a strike by fighting terror at its source), which is the traditional case, and a quasi-private good, namely, each potential target pays for its own security.

The dual nature of anti-terrorist investments reflects itself also in the two types of externalities that spending on local security generates. The first is zero-sum; conditional on a strike taking place, an extra dollar spent by a particular target on the *L*-strategy decreases the probability of a strike against that target, and thereby it necessarily increases the probability of other potential targets being hit. That is, enhancing the security of a particular target confers a negative externality on all other potential targets. On the other hand, an extra dollar spent on one's own security has some deterrence effect because it lowers the probability that terrorists will choose to strike and hence confers a positive externality. Thus, enhanced security at any particular target reduces the attractiveness of striking in general, and hence lowers the likelihood of

an attack for everybody. The model shows that, on the whole, the externalities generated by extra spending on own security of particular targets are negative; that is, the net impact of enhancing the security of a particular target is to increase the risk faced by others.

The two alternative strategies (*S* versus *L*) differ greatly also in their relative effectiveness. The per-dollar benefits to society of devoting resources to fighting terrorism at the source, which constitutes a public good, are much larger than those derived from enhancing the security of individual targets, measured in terms of the reduction in the probability of a terrorist strike. In fact, it can be shown that the difference is on the order of *N*, the number of potential targets; i.e., the *S*-strategy is about *N times* as effective as the *L*-strategy.[26] This finding is hardly surprising, but the magnitude of the difference is sobering.

These inferences provide the background for one of the key questions that arise in this context: how much should the government invest in the *S*-strategy, assuming that its goal is to minimize the expected value of losses from a terrorist attack, and taking into account the behavior of the other parties to the game (i.e., the optimizing behavior of terrorists, on the one hand, and of potential targets, on the other)? The model provides a clear answer: *the government should spend on fighting terrorism at its source as much as it takes to induce private targets to spend* nothing *on local security.*[27] Recall that spending on the *S*-strategy reduces *p*, the probability that a terrorist strike will take place. Thus, the optimal rule is that the government should decrease *p* (via expenditures on the *S*-strategy) to the point where individual targets find it too costly to invest in their own (local) security.[28]

Ideally then, we should see large amounts of resources being spent on intelligence and related *S*-strategy activities, and *none* on the *L*-strategy. In practice, though, we see large and increasing amounts being spent on local security. That may be so for two reasons: (1) the government does not spend enough on the *S*-strategy, and (2) individual targets overestimate the probabilities that they will be hit or otherwise attach additional psychological benefits to local security that go beyond the stark logic of our models.[29] Additional research is needed to elucidate these issues.

Finally, the model can also be deployed to explore the relative efficiency of R&D aimed at either strategy, which can be thought of in the present context as innovative activity aimed at increasing the effectiveness of spending on security. That is, R&D in the context of the *S*-strategy is seen as increasing the extent to which investments in

fighting terrorism at its source reduce the probability of a strike, and similarly, R&D in the context of the *L*-strategy increases the extent to which spending on local security reduces the probability of particular targets being hit. The analysis shows that R&D devoted to the *S*-strategy is likely to be much more effective than R&D aimed at the *L*-strategy, provided only that *total* expenditures on fighting terrorism at the source are larger than the *average* expenditure on one's own security by individual targets, which is surely the case.

V. R&D to Fight Terrorism—Policy Implications

The dual nature of defense in the context of the war against terrorism also figures in the allocation of resources to R&D: should the government engage in and/or pay for R&D aimed at improving the means available both to fight terror at its source and to protect the population from its consequences? First, we know that even in the context of purely private goods, a market economy may well underinvest in R&D. The fact that R&D generates spillovers implies that the social rate of return is typically higher than the private return, and hence that private investment in R&D may fall short of the socially desirable level. Thus, even if providing security from terrorism was deemed to be entirely a private good, there would be room for government support for anti-terrorism-related R&D, for example in the context of the advanced technology program (ATP).

As we have seen, though, there is a component of the fight against terror that clearly has a public good nature, which is the one associated with the *S*-strategy, that is, security outlays aimed at diminishing p, the likelihood of a terrorist strike. This involves locating, monitoring, and intercepting terrorist cells around the world; disrupting their logistical and financial base; limiting their access and mobility; and so forth, so that the ability or readiness of terrorists to carry out attacks are impaired as much as possible. Therefore, R&D aimed at enhancing the effectiveness of these outlays should be the government's responsibility, much as the provision of traditional national security–related R&D has always been.[30] One of the key aspects of the *S*-strategy is intelligence, that is, the gathering of information on terrorists (masterminds, operatives, and supporters), their modes of operation and sources and channels of finance, and (above all) as much detail as possible on their future plans. As noted in Section III, one of the distinguishing features of the terrorist threat is the generalized, diffused nature

of it, that is, the fact that there is a great deal of inherent uncertainty regarding where and when terrorists will strike. Intelligence broadly means the reduction of such uncertainty. It conveys vast, generalized benefits, and therefore it is the crucial tool and the pre-eminent public good in the context of the fight against terror. R&D aimed at providing better intelligence capabilities has therefore very high social payoffs, suggesting that it should be made the cornerstone of R&D policy in the war against terrorism.

In terms of R&D aimed at the *L*-strategy, there may be a role for the government, even though it is quite likely that local security would be provided privately because, as already mentioned, the market may still underinvest in R&D for the usual reasons.[31] Furthermore, there is certainly a role for the government in promoting basic research that feeds into down-the-line R&D aimed at enhancing local security, much as it does for most basic research in almost all areas of science and technology. Since Arrow (1962), it is well understood that basic research generates the most spillovers, the benefits from it are inherently very hard to appropriate, and hence it is up to the government to promote and subsidize it.

There are two additional areas that also call for a government role: R&D aimed at protecting from nonconventional terrorist threats (see appendix 1.3) and R&D for improved cyber security. The former differs from a conventional terrorist threat obviously in the scope of the potential damage, making them "macro" threats and thus turning the provision of security against them into a classic public good, with the usual implications. With the proliferation of Internet-based or interconnected computerized infrastructure systems, threats at computer and communications networks have acquired once again a "macro" dimension (again, because of the scope and reach of the damage that may be inflicted), and therefore it is up to the government to play a key role in confronting these threats, particularly in the conduct of R&D.

Beyond R&D in purely technological fields, research in the behavioral and social sciences may also play a significant role in confronting terrorism: first, in understanding the motivations, the psychological makeup, and the wider sociological context of terrorists, as well as contributing cultural, political, and economic factors; and second, in dealing with the psychological and socioeconomic effects of the terrorist threat on the targeted population, including the perception of probabilities, which influences in turn the incentives to invest in local security.

VI. Defense R&D: Technological Directions and Market Competition

Both intelligence and protection of potential targets require the development of sensory computer interfaces that can be used for detection and intelligence gathering. As the analysis above suggests, increasing detection capabilities (in the broad sense) should be one of the main goals of defense R&D. The protection of targets as well as the identification of suspects requires enhanced ability to detect weapons, explosives, bacteriological materials, and other potentially dangerous devices being carried by individuals, shipped over different means of transportation, stored in hidden places, etc. It also requires positive identification of individuals, both suspects and those with legitimate access permits to designated places.

These screening and detection capabilities should allow for the fast and reliable screening of people, containers, and luggage with minimal disruption to economic activity, travel, and privacy. This is a tall order, considering the staggering number of people moving daily through airports and other transport modes and entering big office buildings, government offices, and infrastructure facilities, and the number of containers shipped, parcels mailed, and so forth. Another set of capabilities that need to be enhanced are those related to eavesdropping and interception of all sorts of communications, ranging from those taking place over regular phone lines anywhere in the world to conversations inside caves in eastern Afghanistan or in underground parking lots in New York.

The common denominator of this vast array of required capabilities is that one needs to be able to emulate human senses (to "hear," to "see" and "recognize," to "smell," to "touch and feel") in automated, computerized ways. That is, one needs to create smart, sensory interfaces between computerized detection systems and the physical world that will be able to activate those senses in fast, reliable ways as a matter of routine.[32] I emphasize this required change in the direction of technical change (i.e., emulating human sensory perceptions) because in fact computer technology has developed historically in a very asymmetric, skewed way vis-à-vis human capabilities. It sought relentlessly to improve the "brain" (i.e., the central processor), while keeping a primitive sensory interface. Call it the "Helen Keller model" of computer technology: virtually deaf, dumb, blind (and lacking also sense of touch or smell), but highly intelligent (i.e., capable of performing enormous

amounts of routine computations). This development has been, on reflection, a very peculiar path of technological progress, dictated in part by the constraints of scientific knowledge but also by the predominant type of uses for computers.

There is, however, increased recognition that developing computerized sensory interfaces is extremely important for a wide and rapidly expanding array of civilian uses, ranging from automobiles (e.g., voice-activated computerized commands, improved safety technologies, preventive maintenance, etc.) to medicine and consumer appliances and gadgetry. Development of computerized sensory interfaces is in fact one of the technological frontiers attracting a great deal of attention, both in basic and applied research. Thus, defense R&D devoted to this area is very likely to have immediate, direct spillovers to civilian uses. Presumably, there have been spillovers from "traditional" defense R&D all along (even if these spillovers are hard to quantify). The difference is that, in this case, the technological frontier that defense (anti-terror) R&D is supposed to breach is the same as that required for progress in civilian uses. That is not the case with, say, improvements in nuclear weapons or in stealth technology. In these cases, the gradient of technological advance in military R&D has no direct relevance for civilian purposes, and the spillovers, if any, are only indirect.

Another area that calls for increased R&D resources is fast analysis of vast amounts of information (referred to as "fusion"), as best exemplified by the need to review staggering amounts of voice, data, and email messages intercepted by the National Security Administration (NSA) and other agencies. It would seem that the rate of growth of communications (i.e., the amount of messages being transmitted over an expanding range of modes: fixed line and cellular phones, satellites, the various wireless modes, fax and email) is at least as fast if not faster than the rate of improvement in computer capabilities aimed at analyzing them. Thus, to shorten substantially the delays in reviewing these communications (which have proven critical for the ability to identify terrorist threats in real time), the technologies in question would have to undergo significant breakthroughs. Again, this gradient of technological progress fits also well-defined civilian needs, for example, in terms of the data analysis requirements associated with the genome project and its aftermath (and even more so the corresponding program for mapping proteins) or more generally "data mining" in businesses that have become an increasingly important activity in a wide range of sectors.

What is required then is the setting up of R&D programs that would support mainly the development of sensory computer interfaces for detection and intelligence gathering and of computer technologies for massive data analysis. As already mentioned, the systems sought are, for the most part, "dual use" in the sense that they have both defense and civilian applications.[33] This is very different from Cold War defense R&D, which was aimed primarily at big weapons systems. As for the overall budget for defense R&D, the point emphasized here is the internal reallocation required, away from big weapons systems and toward the new programs. It remains to be seen how the total would be affected.

The different nature of the new defense R&D may have profound implications for the industrial organization aspects of the sectors involved. The development of big weapons systems in the decades of the Cold War led to a high concentration of both R&D and procurement in a few large corporations, thus conferring on them a great deal of market and bargaining power. It is quite likely that this course had detrimental effects in terms of costs and efficiency, and it may have steered technical advance into questionable directions (such as with the extremely expensive stealth technology). By contrast, the development of sensory computer interfaces, computer technologies for massive data analysis, Internet security, biological protection, and the like, entails an entirely different playing field. These systems are by and large dual use; a private market exists for many of the products sought; and already a vast number of players work in the high-tech, computer, and biotech sectors that can partake in this new R&D, and it can attract new entrants. R&D programs designed to preserve this diversity and to encourage further competition may prove highly beneficial both for the required defense R&D and for the advanced sectors of the economy themselves, thus fostering economic growth.

VII. Conclusion

The foregoing analysis of the threats facing the United States in the wake of September 11, 2001, suggests the articulation of a coherent defense R&D policy based on the following set of principles:

1. It is no longer clear whether it is still justified to devote large amounts of R&D to the development of costly big weapons systems, such as new jet fighters; nuclear subs; heavy payload, long-range missiles; carriers; etc. Gradual upgrades of existing systems and basic research for future generations of these systems may suffice.[34] The resources thus saved could be reallocated to the development of intelligence and anti-terrorist means.

2. The war against terrorism involves two main aspects: fighting terrorists at their source (the *S*-strategy) and protecting potential targets (the *L*-strategy). The former is a pre-eminent public good and hence should be supplied by the government, whereas the latter is typically a private or a local public good that carries negative externalities and is far less efficient than fighting terrorism at the source. Formal analysis indicates that the government should devote enough resources to the *S*-strategy to dissuade potential targets from spending on their own security, at least when the costs of financing such spending are linear. The different nature of each strategy dictates also the kind of R&D needed.

3. Resources devoted to the *S*-strategy involve monitoring and intercepting terrorist cells around the world, disrupting their logistical and financial base, and limiting their access and mobility to impair their ability to carry out attacks (i.e., decreases in p). This involves first and foremost intelligence activities in their broadest sense, suggesting that the most important goal of defense R&D should be to provide advanced technological means and thus enhance the intelligence capabilities of the various U.S. agencies in charge (primarily the CIA and the NSA) and of the supporting military forces.

4. Protecting potential targets is a mixed public-private good and, accordingly, the private sector is likely to provide some of the required security. If they do so, private firms will also have incentives to conduct R&D aimed at developing more effective means to provide local security. However, that incentive may not be strong enough for the usual reasons; moreover, the conduct of the required basic R&D necessitates government support, as is the case in almost all realms of science and technology.

5. R&D aimed at protecting from nonconventional terrorist threats and R&D for cyber security also call for an active government role. The former constitutes "macro" threats; therefore, the provision of security against those threats can be seen as a classic public good, with the usual implications. With the proliferation of interconnected computerized infrastructure systems, threats at computer and communications

networks have also acquired a "macro" dimension, and therefore it is up to the government to play a leading role, particularly in the conduct of R&D, in confronting them. There is also room to encourage research in the behavioral and social sciences, with the aim of understanding both the enemy and the effects of the terrorist threat on the targeted population.

Notes

Prepared for the conference on Innovation Policy and the Economy, Washington, April 15, 2003. I am thankful to Alon Eisenberg and Marina Tsirulnik for excellent research assistantship; to Guy Kaplan for offering his military expertise; and to Jacob Glazer, Dan Peled, Oren Setter, and Nadine Baudot-Trajtenberg for useful comments.

1. At the beginning of the Cold War, the share of GDP devoted to R&D was just 1.4 percent (in 1953). It rose rapidly during the late 1950s to over 2 percent, and it has fluctuated since within the 2.3 to 2.9 percent range. See the National Science Foundation report at http://www.nsf.gov/sbe/srs/infbrief/nsf03307/start.htm#fig2.

2. For an overview of the economics of defense R&D, see Lichtenberg (1995).

3. A further goal was containment of the Soviet influence around the world, but it is less clear how that goal influenced defense R&D.

4. See, for example, the various treaties restricting the development, testing, and/or deployment of various weapons systems, such as antiballistic missiles (ABMs).

5. For example, in the early 1980s, a full 75 percent of federal outlays on defense R&D went to missiles and aircraft, two of the main items in the category of "big weapons systems" (see Mowery and Rosenberg 1989).

6. Hence the lack at present of effective defensive systems for the missile threats posed by Iraq, Iran, and North Korea. The Patriot system did not perform well during the 1991 Gulf War, and it remains to be seen if the newly developed Israeli Arrow system or the improved Patriot will do better.

7. I refer here just to the technological capabilities as manifested in the quality and effectiveness of the weapons systems, and not to the military stock, that is, the actual quantity of weapons (and manpower) available.

8. R&D (or "knowledge") stock is a widely used concept (see, e.g., Griliches 1984), paralleling that of physical capital stock, and can be computed simply by accumulating lagged R&D expenditures and assuming a given depreciation rate, usually significantly higher than that for physical capital. It is not clear what rate would be appropriate for computing a defense R&D stock; presumably it varies inter alia with the intensity of the arms race. Here, I use a depreciation rate of 15 percent (which has become a sort of focal figure in this type of computation), but I compute the stocks also for a 5 percent rate to gain an idea of the range of uncertainty in that respect.

9. Note that Russia's GDP is at present just about 1/40 that of the United States.

10. Thus, we exclude Canada and Italy.

11. One can argue that R&D costs in China are significantly lower than in the United States, and hence matching the real amount of resources allocated by the United States to defense R&D would entail significantly less than that. However, even if R&D costs were *half* as high in China, that would still entail allocating 2 percent of GDP to military R&D, again a staggering amount. To put that figure in perspective, notice that the share of China's GDP devoted to *total* military expenditures was 1.4 percent in 2001 according to official Chinese figures, or 2.1 percent according to SIPRI (2002).

12. We sorted the items by the allocated budget and examined the items from the top down. Thus, although we classified only about 50 percent of the items, they account for about 90 percent of the total budget.

13. Not all of it is related to anti-terrorism, but we could not make that distinction.

14. There is only one item that explicitly mentions the war on terrorism. "Combating Terrorism Technology Support," Office of the Secretary of Defense, allocated just $49 million in 2003.

15. As David Gold writes in SIPRI (2002), "The F-22 . . . was designed during the cold war to counter an expected new generation of Soviet aircraft and air defenses that never materialized. The F-15, which the F-22 will replace, gives the USA air superiority over any conceivable enemy well into the future. Thus, the F-22 may be a system without a threat to combat. . . ." Estimates predict that a fully equipped plane will cost well above $100 million.

16. Still, in nominal dollar terms, intelligence and anti-terrorist R&D increased by over 50 percent from fiscal year 2001 to fiscal year 2003.

17. It is also very different than previous instances of terrorism, particularly because most terrorist organizations operated locally (within their own countries), and they had as goals igniting some sort of drastic *internal* political change.

18. We follow Arrow (1962) in the sense that the role of R&D and of government policy in this regard should follow from an understanding of the nature of the "good" in question. Arrow dissected the nature of knowledge and of knowledge creation, whereas here we are trying to understand the peculiarities of the war against terror as opposed to conventional warfare, and derive from it the contours of an appropriate defense R&D policy.

19. Consider, for example, what it would have taken to prevent September 11, 2001, had the Federal Bureau of Investigation (FBI) known in advance of the plan: a score of arrests in several locations, conducted by a few hundred agents—a trivial operation relative to the magnitude of the threat.

20. We do not deny, of course, the role of surprise. When poised to launch the offensive on the Nazis, the Allies invested great efforts in deception, that is, in creating uncertainty about where and when D-Day would take place. Yet it is hard to imagine that any outcome of significance for the war depended on the success of the deception campaign.

21. See, for example, Gold (1999) for a discussion of defense as a public good in the international context.

22. In addition, the provision of some public and quasi-public goods entails indivisibilities, that is, minimal large-size investments in production, like that with mass transport, dams, etc.

23. But there may also be positive externalities, as in any other security context. See, for example, Ayres and Levitt (1998).

24. Distributional considerations refer to the fact that public places catering to low-income segments of the population may invest little in security, and thus they become more likely targets. Such an outcome may be perceived as unfair, however, like denying medical care to those unable to pay for it.

25. For antecedents to this type of modeling, see Enders and Sandler (1995).

26. To recall, N stands for the number of potential targets, and hence it may be very large indeed (tens of thousands? hundreds of thousands?).

27. This result refers to the case where the costs of financing the S-strategy are linear, that is, when each additional dollar "costs" the same regardless of how much one spends. However, if it gets increasingly costly to finance spending on the S-strategy (for example, if the government has to resort to more distortionary taxes or to borrowing at increasingly higher interest rates), then one may obtain a solution by which the optimal spending on the S-strategy stops short of nullifying the incentives of potential targets to spend on the L-strategy.

28. Note that in the classic case of a public good (such as national defense), the government has to supply it because there are *no* private incentives to do so (at least not in the required quantities). By contrast, in the present case the government has to allocate enough resources to the public good to *prevent* private agents from spending on local security because such spending is highly inefficient.

29. In addition to the qualification set forth in footnote 27, it may be that increasing costs of financing at the margin effectively cap spending on the S-strategy at levels that still leave room for private spending on the L-strategy. This is a rather unlikely scenario, however, in view of the fact that spending on S-strategy-related activities constitutes a very small fraction of the federal budget.

30. As with traditional national security, that does not necessarily mean R&D should be performed by government agencies, nor that the government should necessarily pay for all or most of the R&D costs. As long as the government commits to purchasing the security products that result from the R&D, private suppliers may share the R&D costs and the associated risks.

31. This is true in spite of the fact that, as mentioned in Section IV, the level of spending in local security should be zero, provided that the government spends enough on the S-strategy.

32. See for example Appendix 1.3: "A collaborative effort . . . will investigate the reliable identification of specific individuals, even when attempts have been made to alter appearance, by measuring the "biometric" signatures of people passing through, for example airports. The effort will range from development of surveillance sensors to algorithms that interpret their data and automatically alert operators to potentially dangerous people."

33. See Cowan and Foray (1995), Lerner (1992), and Molas-Gallart (1997).

34. As R&D progresses from basic research toward development, the costs normally increase rapidly, and hence restricting R&D to the more basic stages would save large amounts of resources.

References

Arrow, Kenneth J. 1962. "Economic Welfare and the Allocation of Resources for Inventions." In R. Nelson, ed., *The Rate and Direction of Inventive Activity*. Princeton, NJ: Princeton University Press, 609–25.

Ayres, Ian, and Steven Levitt. 1998. "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack." *Quarterly Journal of Economics*, February 113(1): 43–77.

Cowan, Robin, and Dominique Foray. 1995. "Quandaries in the Economics of Dual Technologies and Spillovers from Military to Civilian Research and Development." *Research Policy* 24: 851–68.

Enders, Walter, and Todd Sandler. 1995. "Terrorism: Theory and Applications." In K. Hartley and T. Sandler, eds., *Handbook of Defense Economics*, Vol. 1. Amsterdam: Elsevier Science B.V., 213–49.

Gold, David. 1999, January. "Does Military R&D Generate International Public Goods?" Mimeo, *United Nations Department of Economic and Social Affairs*.

Griliches, Zvi, ed. 1984. *R&D, Patents and Productivity*. Chicago, IL: University of Chicago Press.

Hoge, James F., and Gideon Rose, eds. 2002. *The War on Terror*. New York: Council on Foreign Relations Press.

Lerner, Joshua. 1992, August. "The Mobility of Corporate Scientists and Engineers Between Civil and Defense Activities: Implications for Economic Competitiveness in the Post–Cold War Era." *Defense Economics* 3(3): 229–42.

Lichtenberg, Frank. 1995. "Economics of Defense R&D." In K. Hartley and T. Sandler, eds., *Handbook of Defense Economics*, Vol. 1, Amsterdam: Elsevier.

Molas-Gallart, Jordi. 1997, October. "Which Way to Go? Defense Technology and the Diversity of 'Dual-Use' Technology Transfer." *Research Policy* 26: 367–85.

Mowery, David, and Nathan Rosenberg. 1989. *Technology and the Pursuit of Economic Growth*. Cambridge: Cambridge University Press.

SIPRI. 2002. *SIPRI Yearbook 2002: Armaments, Disarmament and International Security*. Oxford: Oxford University Press: 251, 309–22.

Trajtenberg, Manuel. 2003, May. "Defense R&D Policy in the Antiterrorist Era." *Foerder Institute of Economic Research*, WP 11.

U.S. Government, Office of the Under Secretary of Defense (Comptroller), Department of Defense Budget, Fiscal Year 2003. 2002, February. Washington D.C. Available at <http://www.dod.gov/comptroller/fy2003budget/>.

U.S. Government, Executive Office of the President of the United States, Office of Science and Technology Policy. 2003a. FY 2003 R&D Budget Documents. Analytical Perspectives: R&D Chapter, Budget of the United States Government, Fiscal Year 2003. Available at <http://www.ostp.gov/html/ap08.pdf>.

U.S. Government, Executive Office of the President of the United States, Office of Science and Technology Policy. 2003b. FY 2003 R&D Budget Documents. Antiterrorism S&T. Available at <http://www.ostp.gov/html/AntiTerrorismS&T.pdf>.

Appendix 1.1

Defense R&D expenditures: 1991–2000 (billions of constant 1998 dollars)

	United States		Germany		France		United Kingdom		Japan		Russia	
	$	% GDP	$	% GDP	$	% GDP	$	% GDP	$	% GDP	$	% GDP
1991	41.04	0.59	1.77	0.140	6.13	0.47	4.47	0.38	1.56	0.05	1.96	0.34
1992	43.74	0.59	2.18	0.108	4.99	0.38	4.67	0.39	1.80	0.045	1.87	0.36
1993	36.59	0.49	0.73	0.036	3.22	0.24	3.74	0.30	1.82	0.045	1.66	0.36
1994	38.64	0.5	1.87	0.089	3.74	0.28	2.70	0.21	1.83	0.05	1.19	0.29
1995	37.61	0.48	1.25	0.06	4.36	0.32	3.22	0.25	1.85	0.045	1.27	0.35
1996	34.59	0.43	0.93	0.044	3.95	0.29	3.64	0.27	1.88	0.045	0.92	0.29
1997	38.75	0.46	2.18	0.106	2.70	0.19	3.43	0.25	1.89	0.045	1.35	0.30
1998	35.80	0.40	2.18	0.099	2.18	0.15	3.01	0.21	1.89	0.05	1.16	0.42
1999	35.43	0.39	1.79	0.079	2.91	0.19	3.26	0.22	1.89	0.05	1.26	0.32
2000	34.97	0.38	1.76	0.079	2.88	0.19	3.30	0.22	1.90	0.05	1.41	—

Sources: *G7 countries*: Defense R&D computed from data taken from the National Science Foundation, Division of Science Resources Statistics (NFS/SRS), Appendix Table 5-41, and from SIPRI Yearbook 2002 (for total military expenditure).
Japan: Defense R&D expenditures estimated as comprising 5 percent of total military expenditure.
For 1999–2000, all countries other than the United States: Extrapolation is based on mean (defense R&D/total military expenditures) ratio for 1996–1998.
Russia: Total military expenditures come from SIPRI (2002). For defense R&D as percentage of defense budget, see Ministry of National Defense, Republic of Korea (www.mnd.go.kr). GDP comes from the World Bank and IFS. For 1992–1993, extrapolation is based on the mean (defense R&D/total military expenditures) ratio for 1994–1996. For 1991, extrapolation is based on mean (defense R&D/GDP) ratio for 1992–1994.
See also U.S. Government (2003a).

Appendix 1.2

Sample list (twenty top items) from the Defense Department RDT&E programs[a]

Organization name	Project name	Category[b]	2003 budget
Ballistic Missile Defense Organization	Ballistic Missile Defense Midcourse Defense Segment	D	3,195,104
Air Force budgeted by DOD	Joint Strike Fighter EMD	B	1,743,668
Navy budgeted by DOD	Joint Strike Fighter (JSF)—EMD	B	1,727,500
Ballistic Missile Defense Organization	Ballistic Missile Defense System Segment	D	1,065,982
Ballistic Missile Defense Organization	Theater High-Altitude Area Defense System—TMD, EMD	D	932,171
Army budgeted by DOD	Comanche	B	914,932
Air Force budgeted by DOD	Advanced EHF MILSATCOM (space)	BI	825,783
Air Force budgeted by DOD	Space Based Infrared Systems (SBIRS) High EMD	I	814,927
Ballistic Missile Defense Organization	Ballistic Missile Defense Boost Defense Segment	D	796,927

Appendix 1.2

(continued)

Organization name	Project name	Category[b]	2003 budget
Navy budgeted by DOD	SC-21 total ship system engineering	B	717,397
Air Force budgeted by DOD	F-22 EMD	B	627,266
Defense Advanced Research Projects Agency	Materials and electronics technology	M	440,500
Defense Advanced Research Projects Agency	Computing systems and communications technology	MI	424,940
Navy budgeted by DOD	V-22A	B	420,109
Air Force budgeted by DOD	Test and evaluation support	M	398,266
National Security Agency	Information systems security program	I	394,257
Navy budgeted by DOD	Defense research sciences	M	393,557
Ballistic Missile Defense Organization	Ballistic Missile Defense Sensors	D	373,447
Air Force budgeted by DOD	NAVSTAR Global Positioning System (space and control segments)	BI	324,098

[a] Ranked according to the 2003 budget allocations.

[b] Categories: B—big weapons systems, I—intelligence, T—anti-terrorism, M—miscellaneous, D—ballistic missile defense. Two letters (such as "BI") mean that the item is deemed related to both categories; in the calculation of expenditure shares per category, the expenditure is then split in half.

Source: U.S. Government (2002).

Appendix 1.3: OSTP, Fiscal Year 2003 R&D Budget Documents—Anti-Terrorism S&T

The President is committed to leveraging the capabilities of our nation's scientific and engineering communities in countering new threats to our homeland and our national security. The President's 2003 Budget represents an escalation in the Administration's strong support for research and development aimed at defeating these dangers to our way of life. Research and development funding for homeland security and combating terrorism (including protecting critical infrastructure) will rise from nearly $1 billion in 2002 to an estimated $3 billion in 2003. These funds will be used to develop new or improved capabilities for protecting our nation from terrorism and its consequences. Some examples are provided below.

Confronting Weapons of Mass Destruction

The Office of Homeland Security has coordinated a major multi-agency research effort that will lead to improved techniques for timely detection of biological attacks on our nation, and for minimizing the consequences of an attack. In the Department of Health and Human Services and Department of Defense (DOD), funding for bioterrorism R&D is increased from a pre-9/11 level of just over $300 million to more than $2.4 billion—more than a factor of seven increase. $1.75 billion is provided to the National Institutes of Health (NIH) to perform fundamental research leading to the development of rapid identification and monitoring technologies, diagnostic tests, new vaccines and therapeutics, including an improved anthrax vaccine. An additional $49 million would be provided to the Food and Drug Administration (FDA) for research and drug approval. Aside from a variety of other research activities, the DOD will dedicate $420 million to ensure rapid detection of biological agents, devise countermeasures, and to study and model the technology and tactics of bioterrorists. The Environmental Protection Agency (EPA) will receive $75 million to develop improved techniques and procedures for coping with biological and chemical incidents. Additionally, investments are being made to enhance the nation's capability for detecting the use of chemical and radiological weapons. The Department of Energy (DOE), for example, will demonstrate a multi-station prototype of a chemical agent detection and response system in the Washington, D.C., Metro system.

Detecting Potential Danger

A collaborative effort between the Department of Justice, the Federal Bureau of Investigations, the National Institute of Standards and Technology (NIST), and DOE will investigate the reliable identification of specific individuals, even when attempts have been made to alter appearance, by measuring the "biometric" signatures of people passing through, for example, airports. The effort will range from development of surveillance sensors to algorithms that interpret their data and automatically alert operators to potentially dangerous people.

Explosives Detection

The Federal Aviation Administration, DOE, and the Technical Support Working Group (jointly sponsored by the State Department and DOD) will research improved methods for detecting conventional explosives in luggage, in airports and other transportation portals, at the borders, and in high population density areas.

Setting Standards

There will be a coordinated multi-agency effort for setting appropriate standards in homeland security; these agencies include NIST, EPA, the Centers for Disease Control and Prevention, and the Nuclear Regulatory Commission. Areas of focus will include setting standards for equipment used by first responders, and setting decontamination thresholds for determining when an area can be reoccupied after an attack.

Basic Research

Fundamental investigative efforts will be funded at several agencies to provide basic scientific data for the war against terrorism. These efforts include $27 million for fundamental work at the National Science Foundation for sequencing the genomes of pathogens, so that more effective detection schemes and defenses might be developed, and work at NIH on developing candidate products that could become the next generation of vaccines.

Source: U.S. Government (2003b).